

**CLAIM AMENDMENTS**

This listing of claims will replace all prior versions and listings of claims in the application.

**Listing of Claims**

1. (Currently Amended) A method of detecting denial of service (DoS) attacks in an Internet accessible network having at least one proxy server incorporating a session initiation protocol (SIP), ~~said SIP including session initiation protocol~~ includes INVITE (~~INV~~) messages that request set-up of an Internet telephone call and ~~SIP-180 Ringing message messages that indicate ringing, the method~~ comprising the following steps of:

aggregating said INVITE messages and said 180 Ringing messages for all users on said Internet accessible network;

detecting an imbalance between an accounting a number of said SIP-INVITE and SIP-180 Ringing-message messages resulting from a denial-of-service DoS attack; and

providing an indication of the presence of a current DoS attack on said proxy server based on detection of said imbalance.

2. (Currently Amended) The method of ~~detecting denial of service attacks in an Internet accessible network as defined in claim 1.~~

wherein ~~a number~~ ~~the number~~ (H) of INVITE messages including credentials that are sent from a user client in response to an authentication required (407) message from the proxy server, said credentials being information used by the proxy server to authenticate the INVITE messages, are removed from the accounting before the balance is tested such that when the equation:

$$\text{INV}_o \text{ [[to]]} + \text{INV}_c - H = N_{180}$$

where  $\text{INV}_o$  is the number of INVITE messages without said credentials,  $\text{INV}_c$  is the number of INVITE messages with said credentials, and  $N_{180}$  is the number of said 180 messages, is not true within a predetermined margin of error, then the presence of a ~~denial of service~~ DoS attack on the proxy server is indicated by the inequality.

3. (Currently Amended) The method of ~~detecting denial of service attacks in an~~ Internet accessible network as defined in claim 2, further including the following step:

causing said proxy server to maintain a call information table for determining the value of H.

4. (Canceled).

1 5. (Currently Amended) A system for detecting denial of service (DoS) attacks  
2 against session initiation protocol elements in a Internet accessible network having  
3 at least one proxy server, said system comprising:

4 means for aggregating said INVITE messages and said 180 Ringing messages  
5 for all users on said Internet accessible network; and

6 means, within wherein ~~said proxy server, includes means for~~ determining if  
7 the number of INVITE messages including credentials (INVc) sent to said proxy  
8 server from user clients in response to an authentication requirement exceeds a  
9 ~~predetermined level~~ number of said 180 Ringing messages that indicates a DoS  
10 attack, said credentials being information used by the proxy server to authenticate  
11 the INVITE messages.

1 6. (Currently Amended) A system for detecting denial of service (DoS) attacks in  
2 an Internet accessible network having at least one proxy server incorporating  
3 session initiation protocol (SIP), said system comprising:

4 means for aggregating said INVITE messages and said 180 Ringing messages  
5 for all users on said Internet accessible network; and

6 means, within wherein ~~said proxy server, includes means for~~ detecting an  
7 imbalance between ~~an accounting a number of SIP~~ said INVITE and ~~SIP~~ said 180

8 | Ringing messages, the imbalance indicating that indicates the presence of a current  
9 | ~~denial of service-DoS~~ attack on said proxy server.

1 | 7. (Currently Amended) The system of A system for detecting denial of service  
2 | ~~attacks against session initiation protocol elements in an Internet accessible~~  
3 | ~~network as claimed in claim 5, wherein said means for determining~~ creates a call-  
4 | info table for use in tracking said INVITE messages.

1 | 8. (Currently Amended) The system of A system for detecting denial of service  
2 | ~~attacks against session initiation protocol elements in an Internet accessible~~  
3 | ~~network as claimed in claim 6, wherein said means for detecting~~ creates a call-info  
4 | table.